9111-14-P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2022-USCBP-2022-0007]

Privacy Act of 1974; System of Records

AGENCY: U.S. Customs and Border Protection, Department of Homeland Security.

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to modify and reissue a current DHS system of records titled, "DHS/U.S. Customs and Border Protection (CBP)-009 Electronic System for Travel Authorization System of Records." The Electronic System for Travel Authorization (ESTA) system is a web-based system used to determine the eligibility of international travelers to travel to the United States under the Visa Waiver Program (VWP).[1] DHS/CBP is updating this system of records to (1) reflect the expansion of the categories of records to include the collection of photographs, (2) clarify the retention schedule, and (3) remove references to the I-94W, "Nonimmigrant Visa Waiver Arrival/Departure Record". The exemptions for the existing system of records notice will continue to be applicable for this updated system of records notice. This modified system of records notice will be included in the DHS's inventory of record systems.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This modified system will be effective upon publication. New or modified routine uses will be effective **[INSERT**

[1] The Visa Waiver Program (VWP), administered by DHS in consultation with the State Department, permits citizens of 40 countries to travel to the United States for business or tourism for stays of up to 90 days without a visa. In return, those 40 countries must permit U.S. citizens and nationals to travel to their countries for a similar length of time without a visa for business or tourism purposes.

DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number USCBP-2022-0007 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Lynn Parker Dupree, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C., 20528-0655.

Instructions: All submissions received must include the agency name and docket number USCBP-2022-0007. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Debra L. Danisek, (202) 344-1610, Privacy.CBP@cbp.dhs.gov, CBP Privacy Officer, Privacy and Diversity Office, 1300 Pennsylvania Avenue, NW, Washington, D.C., 20229. For privacy questions, please contact: Lynn Parker Dupree, (202) 343-1717, Privacy@hq.dhs.gov, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C., 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to update and reissue a current Department of Homeland Security system of records titled, "DHS/United States Customs and Border Protection (CBP)-009 Electronic System for Travel Authorization (ESTA) System of Records." On

August 3, 2007, the President signed into law the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act).[2] Section 711 of the 9/11 Act required that the Secretary of Homeland Security, in consultation with the Secretary of State, develop and implement a fully automated electronic travel authorization system to collect biographical and other information as the Secretary determines necessary to evaluate, in advance of travel, the eligibility of the applicant to travel to the United States under the Visa Waiver Program (VWP), and whether such travel poses a law enforcement or security risk.[3] Prior to implementing the Electronic System for Travel Authorization (ESTA), international travelers from VWP countries were not evaluated, in advance of travel, for eligibility to travel to the United States under the VWP.

DHS/CBP created the ESTA system to collect information from individuals intending to travel under the VWP, as well as representatives who submit information on behalf of the applicant. The ESTA application requests the intended traveler's name, country of birth and citizenship, date of birth, gender, travel document information, contact information (*e.g.,* phone, email address), voluntary submission of social media information, family information, employment information, and destination address, as well as responses to questions related to an applicant's eligibility to travel under the VWP.

Upon submission, DHS/CBP vets the application against selected security and law enforcement databases as well as publicly available sources, such as social media. The results of this vetting help to inform DHS/CBP's assessment of whether the traveler poses a law enforcement or security risk and whether the application should be approved. ESTA authorizations can take up to 72 hours to be complete. However, DHS/CBP is generally able to approve/deny an ESTA authorization within a much shorter time frame.

---

[2] *See* Public Law 110-53.
[3] *See* 8 U.S.C. 1187(h)(3)(A).

If the ESTA application is denied, the applicant is not eligible to travel to the United States under the VWP.[4] If the application is approved, the approval establishes that the applicant is eligible to travel to the United States under the VWP but does not guarantee that he or she is admissible to the United States. Upon arrival to a United States port of entry, the VWP traveler will be subject to an inspection by a CBP officer who may determine that the traveler is inadmissible under section 212 of the Immigration and Nationality Act (INA) and deny entry under the VWP. ESTA travel authorizations are generally valid for two years from the date of authorization, or until the VWP traveler's passport expires, whichever comes first. An ESTA approval provides authorization for the traveler to travel to the United States for multiple trips over a period of two years, generally eliminating the need for a traveler to reapply during the validity period unless the traveler fails to meet the requirements of the VWP, or the ESTA approval is revoked.

DHS/CBP is publishing this modified system of records to make changes for transparency.

DHS/CBP is expanding the category of records to include photographs. As part of the ESTA application process, DHS/CBP collects applicant photographs, which may include both the passport photograph and/or a "selfie," if submitting the ESTA application via the mobile application. As described above, the ESTA application requires several key pieces of biographic information, which can be found on the passport biographic data page (*e.g.,* name, date and place of birth, country of citizenship). Applicants and representatives capture[5] or upload[6] a picture of the passport biographic

[4] Applicants denied a travel authorization to the United States via ESTA may still apply for a nonimmigrant visa from the U.S. Department of State at a U.S. Embassy or Consulate.
[5] To capture a photograph of the passport's biographic data page, the applicant or representative must use a device with a camera, such as an Android or an iOS device.
[6] If a camera is not detected on the device, the applicant or representative has the option to upload a pre-scanned image in .gif, .png, .jpg, or .jpeg file format.

data page to include the photograph or retrieve[7] the photograph from the passports eChip into the application. Applicants (or their representative) submit the passport photograph for identity verification and vetting purposes. DHS/CBP stores the image of the passport biographic data page for identity verification and reconciliation purposes. Photographs retrieved using the passport eChip are compared against a separate "selfie" that is required for mobile application submissions. The "selfie" undergoes a "liveness" test to determine that it is a real person - not a picture of a person.[8] Using CBP's Traveler Verification System (TVS) facial matching algorithms, CBP compares the "selfie" with the passport photograph to conduct a 1-to-1 match to confirm whether the identities in the two photographs match.[9] Photographs, regardless of submission method, are stored in the ESTA system consistent with the ESTA retention schedule.

DHS/CBP is also updating this notice to clarify the retention schedule for the data. The overall retention does not change, but DHS/CBP is more clearly documenting that these records are retained for 15 years.

Finally, DHS/CBP is also removing references to the I-94W, "Nonimmigrant Visa Waiver Arrival/Departure Record," since the I-94W is not processed in ESTA. The I-94W is separately covered under the DHS/CBP-016 Nonimmigrant Information System, 80 FR 13398 (March 13, 2015).

---

[7] If the applicant submits the application through a mobile device, he or she can place the mobile device near the passport's eChip to enable the Near Field Communication (NFC). NFC is used for contactless exchange of data over short distances. Two NFC-capable devices are connected via a point-to-point contact over a short distance. This connection can be used to exchange data between devices.

[8] Liveness detection relies on algorithms to analyze facial images to determine whether the image is of a live human being or of a reproduction of that person (e.g., a photograph of the person).

[9] CBP's TVS is an accredited information technology system consisting of a group of similar systems and subsystems that support the core functioning and transmission of data between CBP applications and partner interfaces. Since early 2017, CBP has used the TVS as its backend matching service for all biometric entry and exit operations that use facial recognition, regardless of air, land, or sea. See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE DHS/CBP/PIA-056 TRAVELER VERIFICATION SERVICE, available at https://www.dhs.gov/privacydocuments-us-customs-and-border-protection.

Consistent with DHS's information sharing mission, information stored in the DHS/CBP-009 ESTA system of records may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/CBP may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

This modified system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/CBP-009 Electronic System for Travel Authorization System of Records.

In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER: Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-009 Electronic System for Travel Authorization (ESTA) System of Records.

SECURITY CLASSIFICATION: Unclassified and classified. The data may be retained on classified networks, but this does not change the nature and character of the data until it is combined with classified information.

SYSTEM LOCATION: Records are maintained at the DHS/CBP Headquarters in Washington, D.C., and field offices. Records are replicated from the operational system and maintained on the DHS unclassified and classified networks to allow for analysis and vetting consistent with the stated uses, purposes, and routine uses published in this notice.

SYSTEM MANAGER(S): Director, ESTA Program Management Office, esta@cbp.dhs.gov, U.S. Customs and Border Protection Headquarters, 1300 Pennsylvania Avenue NW, Washington, D.C., 20229.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title IV of the Homeland Security Act of 2002, 6 U.S.C. 201 *et seq.,* the Immigration and Naturalization Act, as amended, including 8 U.S.C. 1187(a)(11) and (h)(3), and implementing regulations contained in 8 CFR part 217; the Travel Promotion Act of 2009, Public Law 111-145, 22 U.S.C. 2131.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to collect and maintain a record of applicants who want to travel to the United States under the VWP, and to determine whether applicants are eligible to travel to and enter the United States under the VWP. The information provided through ESTA, including information about other persons included on the ESTA application, is vetted against various security and law enforcement databases to identify those applicants who pose a security risk to the United States and to inform CBP's decision to approve or deny the applicant's ESTA application.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Categories of individuals covered by this system include (1) individuals who wish to travel to the United States under the VWP and apply for an ESTA travel authorization and (2) persons, including U.S. citizens and lawful permanent residents, whose information is provided by the applicant in response to ESTA application questions (*e.g.,* point of contact).

CATEGORIES OF RECORDS IN THE SYSTEM: An ESTA application includes:

- Full name (first, middle, and last);
- Other names or aliases, if available;
- Date of birth;
- Country of birth;
- Gender;
- Email address;
- Visa numbers, Laissez-Passer numbers, or Identity card numbers;
- Social media identifiers, such as username(s) and platforms used;
- Publicly available information from social media websites or platforms;
- Telephone number (home, mobile, work, other);
- Home address (address, apartment number, city, state/region);
- Internet protocol (IP) address;
- ESTA application number;
- Global Entry Program Number;
- Country of residence;
- Passport information;
- Department of Treasury Pay.gov payment tracking number information;

- Countries of citizenship and nationality;
- National identification number, if available;
- Address while visiting the United States;
- Emergency point of contact information;
- U.S. Point of Contact information;
- Parents' names;
- Current and previous employer information; and,
- Photograph(s).

The categories of records in ESTA also include responses to questions related to the following:

- History of mental or physical disorders, drug abuse or addiction,[10] and current communicable diseases,[11] fevers, and respiratory illnesses;
- Past arrests, criminal convictions, or illegal drug violations;
- Previous engagement in terrorist activities, espionage, sabotage, or genocide;
- History of fraud or misrepresentation;
- Previous unauthorized employment in the United States;

---

[10] Immigration and Nationality Act (INA) 212(a)(1)(A). Pursuant to INA 212(a), aliens may be inadmissible to the United States if they have a physical or mental disorder and behavior associated with the disorder that may pose, or has posed, a threat to the property, safety, or welfare of the alien or others, or (ii) to have had a physical or mental disorder and a history of behavior associated with the disorder, which behavior has posed a threat to the property, safety, or welfare of the alien or others and which behavior is likely to recur or to lead to other harmful behavior, or are determined (in accordance with regulations prescribed by the Secretary of Health and Human Services) to be a drug abuser or addict.

[11] Consistent with 42 CFR § 34.2, DHS/CBP revised the ESTA application to reflect the current quarantinable, communicable diseases specified by any Presidential Executive Order under Section 361(b) of the Public Health Service (PHS) Act (42 U.S.C. § 264). Executive Order 13295 of April 4, 2003, as amended by Executive Order 13375 of April 1, 2005, and Executive Order 13674 of July 31, 2014, contains the most recent list of quarantinable, communicable diseases. COVID-19 is a quarantinable disease as it falls within the scope of "severe acute respiratory syndromes" which are designated as quarantinable pursuant to Executive Order 13674. As such, COVID-19 was added to the list of diseases an individual must attest to not having to be eligible to travel to the United States.

- Past denial of visa, or refusal or withdrawal of application for admission at a U.S. port of entry;
- Previous overstay of authorized admission period in the United States;
- Travel history and information relating to prior travel to or presence in Iraq or Syria, a country designated as a state sponsor of terrorism, or another country or area of concern;[12] and,
- Citizenship and nationality information, with additional detail required for nationals of certain identified countries of concern.

RECORD SOURCE CATEGORIES: DHS/CBP obtains records from applicants or representatives (*e.g.,* friend, relative, travel industry professional), through the online ESTA application available at https://esta.cbp.dhs.gov/esta/ or a mobile application. As part of the vetting process, DHS/CBP may also use information obtained from publicly available sources, including social media, and law enforcement and national security records from appropriate federal, state, local, international, tribal, or foreign governmental agencies or multilateral governmental organizations to assist in determining ESTA eligibility. This information is stored separate from information collected as part of the ESTA application.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. sec. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including the U.S. Attorneys Offices, or other federal agency conducting litigation or proceedings before any court, adjudicative,

[12] INA 212(a)(12); 8 U.S.C. 1187(a)(12).

or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity, only when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. sec. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another federal agency or federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing,

minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where CBP believes the information would assist enforcement of applicable civil or criminal laws and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

I. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital health interests of a data subject or other persons (*e.g.,* to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk).

J. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS is aware of a need to use relevant data, that relate to the purpose(s) stated in this SORN, for purposes of testing new technology.

K. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate in the proper performance of the official duties of the officer making the disclosure.

L. To a federal, state, tribal, local, international, or foreign government agency or entity for the purpose of consulting with that agency or entity: (1) to assist in making a determination regarding redress for an individual in connection or program; (2) for the purpose of verifying the identity of an individual seeking redress in connection with the operations of a DHS Component or program; or (3) for the purpose of verifying the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

M. To a federal, state, tribal, local, international, or foreign government agency or entity in order to provide relevant information related to intelligence, counterintelligence, or counterterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

N. To the Department of State in the processing of petitions or applications for benefits under the Immigration and Nationality Act, and all other immigration and nationality laws including treaties and reciprocal agreements.

O. To an organization or individual in either the public or private sector, either foreign or domestic, when there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life or property.

P. To the carrier transporting an individual to the United States, prior to travel, in response to a request from the carrier, to verify an individual's travel authorization status.

Q. To the Department of Treasury's Pay.gov, for payment processing and payment reconciliation purposes.

R. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, or in connection with criminal law proceedings.

S. To the Department of Treasury's Office of Foreign Assets Control (OFAC) for inclusion on the publicly issued List of Specially Designated Nationals and Blocked Persons (SDN List) of individuals and entities whose property and interests in property are blocked or otherwise affected by one or more OFAC economic sanctions programs, as well as information identifying certain property of individuals and entities subject to OFAC economic sanctions programs.

T. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: DHS/CBP stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: DHS/CBP may retrieve records by any of the data elements supplied by the applicant or representative.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF

RECORDS: The retention of ESTA records is covered by National Archives and Records Administration DAA-0568-2019-0006. Application information submitted to ESTA, including the photographs, is retained for 15 years. DHS/CBP ingests ESTA application data into other DHS/CBP systems for vetting purposes and is stored in accordance with those system's respective retention periods. For example, ESTA information is ingested into the Automated Targeting System (ATS) and is retained for 15 years and is also ingested into TECS where it is retained for 75 years, consistent with those systems' retention schedules. These retention periods are based on DHS/CBP's historical encounters with suspected terrorists and other criminals, as well as the broader expertise of the law enforcement and intelligence communities. It is well known, for example, that potential terrorists may make multiple visits to the United States in advance of performing an attack. It is over the course of time and multiple visits that a potential risk becomes clear. Travel records, including historical records, are essential in assisting DHS/CBP officers with their risk-based assessment of travel indicators and identifying potential links between known and previously unidentified terrorist facilitators. Analyzing the records for these purposes allows DHS/CBP to continue to effectively identify suspect travel patterns and irregularities. If the record is linked to active law enforcement lookout records, DHS/CBP matches to enforcement activities, and/or investigations or cases (*i.e.,* specific and credible threats; flights, travelers, and routes of concern; or other defined sets of circumstances), the record will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related.

Payment information is not stored in ESTA but is forwarded to Pay.gov and stored in DHS/CBP's financial processing system, Credit/Debit Card Data system, pursuant to the DHS/CBP-003 Credit/Debit Card Data System of Records Notice, 76 FR 67755 (November 2, 2011). When a VWP traveler's ESTA data is used for purposes of

processing his or her application for admission to the United States, the ESTA data will be used to create a corresponding admission record in the DHS/CBP-016 Non-Immigrant Information System (NIIS), 80 FR 13398 (March 13, 2015). This corresponding admission record will be retained in accordance with the NIIS retention schedule, which is 75 years.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS/CBP safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS/CBP has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES: Applicants may access their ESTA information to view and amend their applications by providing their ESTA number, birth date, and passport number. Once they have provided their ESTA number, birth date, and passport number, applicants may view their ESTA status (authorized to travel, not authorized to travel, pending) and submit limited updates to their travel itinerary information. If an applicant does not know his or her application number, he or she can provide his or her name, passport number, date of birth, and passport issuing country to retrieve his or her application number.

In addition, ESTA applicants and other individuals whose information is included on ESTA applications may submit requests and receive information maintained in this system as it relates to data submitted by or on behalf of a person who travels to the United States and crosses the border, as well as, for ESTA applicants, the resulting determination (authorized to travel, pending, or not authorized to travel). However, the Secretary of Homeland Security has exempted portions of this system from certain

provisions of the Privacy Act related to providing the accounting of disclosures to individuals because it is a law enforcement system. DHS/CBP will, however, consider individual requests to determine whether information may be released. In processing requests for access to information in this system, DHS/CBP will review the records in the operational system and coordinate with DHS to ensure that records that were replicated on the unclassified and classified networks, are reviewed, and based on this notice provide appropriate access to the information.

Individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and Headquarters Freedom of Information Act (FOIA) Officer whose contact information can be found at http://www.dhs.gov/foia under "Contact Information." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, Washington, D.C. 20528-0655, or electronically at https://www.dhs.gov/freedom-information-act-foia. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for

notarization. An individual may obtain more information about this process at http://www.dhs.gov/foia or 1-866-431-0486. In addition, the individual should:

- Explain why he or she believes the Department would have information being requested;
- Identify which component(s) of the Department he or she believes may have the information;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

If the request is seeking records pertaining to another living individual, the request must include an authorization from the individual whose record is being requested, authorizing the release to the requester.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: See "Record Access Procedures" above.

NOTIFICATION PROCEDURES: See "Record Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: Pursuant to 6 CFR Part 5, Appendix C, when this system receives a record from another system exempted in that source system under 5 U.S.C. 552a(j) or (k), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here. For instance, as part of the vetting process, this system may incorporate records from CBP's ATS, and all of the exemptions for CBP's Automated Targeting System SORN, described and referenced herein, carry forward and will be claimed by DHS/CBP. As such, law enforcement and other derogatory information covered in this system are exempt from 5 U.S.C. 552a(c)(3)

and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (e)(5), and (8); (f); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, pursuant to 5 U.S.C. 552a(k)(1) and (k)(2): 5 U.S.C. 552a(c)(3); (d)(1), (d)(2), (d)(3), and (d)(4); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f).

DHS/CBP is not taking any exemption from subsection (d) with respect to information maintained in the system as it relates to data submitted by or on behalf of a person, as part of the application process, who travels to visit the United States and crosses the border, nor shall an exemption be asserted with respect to the resulting determination (authorized to travel, pending, or not authorized to travel). However, pursuant to 5 U.S.C. 552a(j)(2), DHS/CBP plans to exempt such information in this system from sections (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information. Further, DHS will claim exemption from section (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(k)(2) as is necessary and appropriate to protect this information. CBP will not disclose the fact that a law enforcement or intelligence agency has sought particular records because it may affect ongoing law enforcement activities.

HISTORY: 84 FR 30746 (June 27, 2019); 81 FR 60713 (September 2, 2016); 81 FR 39680 (June 17, 2016); 81 FR 8979 (February 23, 2016); 79 FR 65414 (November 4, 2014); 77 FR 44642 (July 30, 2012); 76 FR 67751 (November 2, 2011); 73 FR 32720 (June 10, 2008).

*****

Lynn P. Dupree,
Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2022-14789 Filed: 7/11/2022 8:45 am; Publication Date: 7/12/2022]